What is claimed is:

1. A method comprising:

receiving a request for access to a service;

collecting a biometric sample from a user associated with the request;

comparing the biometric sample to a biometric template associated with the user; and

providing access to a private key in accordance with a result of the comparing step.

2. A method according to claim 1, further comprising:

if the result indicates a match, generating a digital signature using the private key to the user.

3. A method according to claim 2, further comprising:

providing the digital signature to the service associated with the request.

4. A method according to claim 1, further comprising:

providing a biometric signature corresponding to the collected biometric sample to the service associated with the request.

5. A method according to claim 4, further comprising:

allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparing step.

6. A method according to claim 1, further comprising:

generating pre-enrollment keys for the user;

supplying the pre-enrollment keys to respective key generators; and

generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators.

7. A method according to claim 6, further comprising:

verifying registration of the user in accordance with a comparison of the final enrollment key;

creating the biometric template for the user only if registration is verified; and

generating the private key only if the biometric template is successfully created.

8. A method according to claim 6, further comprising associating user identification information with the final enrollment key.

9. A method according to claim 1, further comprising:

encrypting the collected biometric sample for transmission to an authentication server; and

including integrity information in the encrypted biometric sample.

10. A method according to claim 9, further comprising:

decrypting the encrypted biometric sample at the authentication server; and

checking the integrity information included with the biometric sample.

11. A method according to claim 9, wherein the integrity information includes a unique transaction identifier.

12. A method according to claim 1, further comprising:

associating user identification information with the private key; and

maintaining a digital certificate containing the user identification information and a public key corresponding to the private key.

13. A method according to claim 1, wherein the biometric sample includes a fingerprint scan.

14. An apparatus comprising:

means for receiving a request for access to a service;

means for collecting a biometric sample from a user associated with the request;

means for comparing the biometric sample to a biometric template associated with the user; and

means for providing access to a private key in accordance with a result of the comparing step.

15. An apparatus according to claim 14, further comprising:

if the result indicates a match, means for generating a digital signature using the private key to the user.

16. An apparatus according to claim 15, further comprising:

means for providing the digital signature to the service associated with the request.

17. An apparatus according to claim 14, further comprising:

means for providing a biometric signature corresponding to the collected biometric sample to the service associated with the request.

18. An apparatus according to claim 17, further comprising:

means for allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with a result of the comparing means.

19. An apparatus according to claim 14, further comprising:

means for generating pre-enrollment keys for the user;

means for supplying the pre-enrollment keys to respective key generators; and

means for generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators.

20. An apparatus according to claim 19, further comprising:

means for verifying registration of the user in accordance with a comparison of the final enrollment key;

means for creating the biometric template for the user only if registration is verified; and

means for generating the private key only if the biometric template is successfully created.

21. An apparatus according to claim 19, further comprising means for associating user identification information with the final enrollment key.

22. An apparatus according to claim 14, further comprising:

means for encrypting the collected biometric sample for transmission to an authentication server; and

means for including integrity information in the encrypted biometric sample.

23. An apparatus according to claim 22, further comprising:

means for decrypting the encrypted biometric sample at the authentication server; and

means for checking the integrity information included with the biometric sample.

24. An apparatus according to claim 22, wherein the integrity information includes a unique transaction identifier.

25. An apparatus according to claim 14, further comprising:

means for associating user identification information with the private key; and

means for maintaining a digital certificate containing the user identification information and a public key corresponding to the private key.

26. An apparatus according to claim 14, wherein the biometric sample includes a fingerprint scan.

27. An authentication infrastructure comprising:

a server that intercepts requests for access to a service; and

a client that collects a biometric sample from a user associated with the request,

wherein the server maintains a biometric template associated with the user for authenticating the collected biometric sample, and

wherein the server provides access to a private key in accordance with a result of the authentication, so that the user need not maintain a token for accessing the service.

28. An authentication infrastructure according to claim 27, wherein the private key is used to sign a message for allowing the user to perform a transaction with the service, the service obtaining a corresponding public key from the server.